附件 1：最佳论文评选申请表

<table>
<tr><td>论文题目</td><td colspan="3">Solving Linear Equations Modulo Unknown Divisors: Revisited</td></tr>
<tr><td>申请人</td><td colspan="3">卢尧</td></tr>
<tr><td rowspan="3">论文作者</td><td rowspan="3">（请全体作者签名）
卢尧，张锐，彭力强，林东岱</td><td rowspan="3">索引机构</td><td>☐ SCI</td></tr>
<tr><td>■ EI</td></tr>
<tr><td>☐ ISTP</td></tr>
<tr><td>期刊/
会议信息</td><td colspan="3">（请给出刊文的期刊或会议的名称，卷、期、页等信息）
ASIACRYPT 2015, LNCS, vol. 9452, pp.189-213. Springer</td></tr>
<tr><td>申请人自述</td><td colspan="3">（请简述论文的目的和意义，解决了什么问题，有何贡献或影响。总字数不超过 500 字）
格规约分析技术是目前为止针对公钥密码算法最有效的攻击手段：攻破了基于背包问题的公钥密码体制；对 RSA 公钥算法最好的分析结果；破解多个基于格的密码算法等等。
我们通过引入新的技术，进一步优化了利用格规约求解模方程小根的分析结果。应用我们的新算法，得到了对多个公钥算法目前为止最好的理论及其实现攻击结果，并对一类基于整数上的全同态方案也有着很好的分析结果。</td></tr>
<tr><td>证明材料清单</td><td colspan="3">（例如：论文评阅人的意见、引用情况、他人评价等）
目前被引 6 次</td></tr>
</table>